IN THE CLAIMS

Please **amend** Claims 1-12 as indicated:

1. (currently amended) A method for establishing a secure connection to a server for a specific user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said method comprising:

storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key ~~and a unique digital certificate~~, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

in response to receiving one of said passwords input from [[a]] the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established between the client computer and the server for the specific user.

2. (currently amended) The method of claim 1, further comprising:

storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

identifying said specific user for opening a keyfile according to said unique identifier.

3. (currently amended) The method of claim 1, further comprising:

authenticating an identity of said specific user through a process of hashing, said process including the steps of:

hashing a message into a hashed message using a hash function;

encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

transmitting said hash function, said message and said encrypted hashed message to said server.

4. (currently amended) The method of claim 1, further comprising prompting said specific user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

5. (currently amended) A client computer for establishing a secure connection to a server for a specific user of the client computer on a network utilizing a Secure Sockets Layer (SSL) system, said client computer comprising:

means for storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key ~~and a unique digital certificate~~, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

means for, in response to receiving one of said passwords input from [[a]] the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established between the client computer and the server for the specific user.

6. (currently amended) The client computer of claim 5, further comprising:

means for storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

means for identifying said specific user for opening a keyfile according to said unique identifier.

7. (currently amended) The client computer of claim 5, further comprising:

means for authenticating the identity of said specific user through a process of hashing, said means for authenticating the identity of said specific user through said process of hashing including:

means for hashing a message into a hashed message using a hash function;

means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

means for transmitting said hash function, said message and said encrypted hashed message to said server.

8. (currently amended) The client computer of claim 5, further comprising means for prompting said specific user for a password through a Graphical User Interface (GUI) in a display associated with said client computer.

9. (currently amended) A computer program product residing on a computer usable medium for establishing a secure connection to a server for a specific user of a client computer on a network utilizing a Secure Sockets Layer (SSL) system, said computer program product comprising:

program code means for storing a plurality of keyfiles for different users in a data storage that is accessible only to a client computer, each of said keyfiles comprising a unique private cryptology key ~~and a unique digital certificate~~, a corresponding public cryptology key, and a name of a Certificate Authority (CA) that issued the unique private cryptology key and the corresponding public cryptology key for a specific user;

program code means for storing a plurality of passwords in said data storage, each of said passwords being associated with a respective keyfile, each of said passwords being capable of opening only one of said keyfiles;

program code means for, in response to receiving one of said passwords input from [[a]] the specific user, opening said one of said keyfiles associated with said one of said passwords and said specific user; and

program code means for transmitting from said client computer to a server a digital certificate from said open keyfile to enable said server to authenticate an identity of said specific user from a plurality of users who are authorized to use said client computer, wherein a secure connection is established between the client computer and the server for the specific user.

10. (currently amended) The computer program product of claim 9, further comprising:

program code means for storing an authentication data for said specific user in said data storage, said authentication data comprising a unique identifier that corresponds to a password for said specific user; and

program code means for identifying said specific user for opening a keyfile according to said unique identifier.

11. (currently amended) The computer program product of claim 9, further comprising:

program code means for authenticating the identity of the specific user through a process of hashing, said program code means including:

program code means for hashing a message into a hashed message using a hash function;

program code means for encrypting said hashed message into an encrypted hashed message using said private cryptology key; and

program code means for transmitting said hash function, said message and said encrypted hashed message to said server.

12. (currently amended) The computer program product of claim 9, further comprising:

program code means for displaying a Graphical User Interface (GUI) in a display associated with said client computer; and

program code means for prompting said <u>specific</u> user for a password through said GUI.